UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/882,491	06/15/2001	Yaron Goland	3382-53699	8148

26119 7590 12/31/2007

KLARQUIST SPARKMAN LLP
121 S.W. SALMON STREET
SUITE 1600
PORTLAND, OR 97204

EXAMINER	
SHAW, YIN CHEN	
ART UNIT	**PAPER NUMBER**
2135	
MAIL DATE	**DELIVERY MODE**
12/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

MN

Office Action Summary	Application No.	Applicant(s)	
	09/882,491	GOLAND, YARON	
	Examiner	Art Unit	
	Yin-Chen Shaw	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/05/2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *2-12* is/are allowed.

6)☒ Claim(s) *1 and 13-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the Request for Continued Examination (RCE) dated on 10/05/2007.
2. Claims 1-2, 13, and 19 have been amended. All other claims are as original.
3. Claims 1-20 have been examined.
4. Claims 1-20 are pending.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 13-18 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al, US Patent No. 6772331B1, hereinafter "Hind", in view of Dondeti et al, US Patent No. 7013389, hereinafter "Dondeti" .

   a. As per claim 13:

   Hind disclose a networked computing device supporting branding to establish cryptographically secured interaction with other deices within a trust group of devices on an open-access network, the networked computing device comprising:

a network interface for communicating on the open-access network, a security initializer operational to receive the branding public key from a branding device securely networked to the networked computing device, and further operational to initialize with the branding public key **[[(Col. 9 lines 25-40 from Hind)]**.

Hind does not expressly disclose the remaining limitation of the claim. However, Dondeti discloses a security resolver operational after being initialized with a branding public key to authenticate trust group membership certificates separate from the branding public key provided to the networked computing device from other devices via the network interface using the branding public key, and further operational to inhibit interaction via the network interface with other devices not authenticated as in the trust group of devices, the security resolver being initially uninitialized **[(Col 10 lines 18-29, and Col 11 line 5 to Col 12 line 20 and Col 6 lines 10-55 from Dondeti)]**; and

the branding device having previously generated the branding public key and trust group membership certificates **[(lines 14-29, Col. 5 from Dondeti)]**.

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Hind's invention to incorporate Dondeti's teaching to implement the group joining between group members without interposing a central authority.

b. As per claim 14:

Hind and Dondeti teach "The networked computing device of claim 13 further comprising: a limited access networking interface; and the security initializer further operational to accept the branding public key when received from the branding device only via the limited access networking interface" in (Col 11 lines 5-45).

c. As per claim 15:

Hind and Dondeti teach "The networked computing device of claim 13 further comprising: the security initializer further operational to accept the branding public key when received from the branding device via the network interface when in an initial unbranded state; and a branding reset operational upon activation to return the security initializer to the initial unbranded state" in (Col 13 lines 35-43).

d. As per claim 16:

Hind and Dondeti teach "The networked computing device of claim 13 further comprising: a branding mode activator operational to place the networked computing device in a branding mode; and the security initializer further operational to accept the branding public key when received from the

branding device via the network interface when in the branding mode" in (Col 11 lines 5-45).

e. As per claim 17:

Hind and Dondeti teach "The networked computing device of claim 13 further comprising: the security resolver further operational when initialized with a trust group membership certificate to provide the trust group membership certificate to other devices via the network interface to attest to membership of the networked computing in the trust group; and the security initializer further operational to receive the trust group membership certificate from the branding device while securely networked to the networked computing device, and further operational to initialize the security resolver with the trust group membership certificate" in (Col 9 lines 15-65, and Col 10 lines 24-30).

f. As per claim 18:

Hind and Dondeti teach "The networked computing device of claim 13 further comprising: the security resolver further operational when initialized with a public/private key pair to encrypt interaction via the network interface with other devices authenticated as in the trust group using the public/private key pair; and the security initializer further operational to receive the public/private key pair from the branding device while securely networked to the networked

computing device, and further operational to initialize the security resolver with the public/private key pair" in (Col 11 lines 5-65).

g. As per claim 20:

Dondeti discloses "The networked computing device of claim 13, wherein: Each trust group membership certificate is sent by an other device and each trust group membership certificates comprises:

a signed name for a trust group (Group Name or group ID);
a signed identifier (host public key, Host ID) for the other devices sending the trust group membership certificate" in (Figure 1, 3); and
"The security resolver is configured to authenticate trust group membership certificates by:

Authenticating, from the trust group membership certificate, the signed name for the trust group and the signed identifier for the other device sending the trust group membership certificate using the branding public key" in (Col 6 lines 10-55); and

Wherein the signed name for a trust group matches the trust group, verifying that the other device sending the trust group membership certificate is a member of the trust group" in (Col 5 lines 1-20).

7. Claims 1 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al, US Patent No. 6772331B1, hereinafter "Hind", in view of Hanna et al., US Patent No. 6801998, hereinafter "Hanna" and Dondeti et al, US Patent No. 7013389, hereinafter "Dondeti" .

a. As per claim 1:

Hind teaches a branding process to establish a trust web of networked computing devices on an open multi-access network, comprising:

securely networking a security-uninitialized device with a branding device via a secured network medium in **[(Col. 9 lines 25-40 from Hind)]**;

initializing the security-uninitialized device, and to provide the security-uninitialized device is a member of the trust web, such that at least some interaction via the open multi-access network with the security-uninitialized device is cryptographically secured to only other devices in the trust web **[(Col 10 lines 18-29, and Col 11 line 5 to Col 12 line 20 and Col 9 lines 35-60 from Hind)]**.

Hind does not specifically disclose other limitations of the claim.

However, Hanna et al. disclose generating group membership and cryptographic key data at the branding, the cryptographic key data for verifying group membership information provided by other devices on the open multi-access network to the security-uninitialized device are

authenticated by the branding device **[(lines 29-51, Col. 5; Figs. 1 and 2a-2b from Hanna)]**;

electronically imprinting the security-uninitialized device with the group membership by transmitting the group membership from the branding device to the security-uninitialized device via the secured network medium **[(lines 54-58, Col. 2; lines 29-51, Col. 5; Figs 1 and 2a-2b from Hanna)]**.

Dondeti discloses the limitation of to use the cryptographic key data to authenticate group membership of other devices interacting with security-un-initialized device on the open multi-access network as a method of joining a un-initialized device into a group by providing a group membership certificate to the un-initialized device. The initialized device with the group membership certificate can send the group membership certificate to other member in the group for authentication **[(Col 4 line 57 to Col 5 line 21 from Dondeti)]**, and from the branding device to the security-uninitialized device transmitting the cryptographic key data **[(lines 22-37, Col. 5 and Fig. 4 from Dondeti)]**.

Hind et al., Hanna et al., and Dondeti et al. are from similar technology relating to security for the digital content and token data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Hind et al. with Hanna et al. and Dondeti et al. since one would be motivated (1) to enhance the network security such that the system is less susceptible to denial of service attacks and attacks by malicious users (lines 39-42, Col. 4 from Hanna et al.) and (2) to incorporate Dondeti's teaching to

implement the group joining between group members without interposing a central authority. Therefore, it would have been obvious to combine Hind et al. with Hanna et al. and Dondeti et al. to obtain the invention as specified in claim 1.

b. As per claim 19:

Dondeti discloses "The branding process of claim 1, wherein the group membership information comprises a certificate signed and generated by the branding device (lines 14-29, Col. 5 from Dondeti) and containing a signed group name as well as signed information naming the security-un-initialized device such that, when the security-un-initialized device provides the certificate to a branded device which is a member of the trust web, the certificate is validated by the branded device, and the branded device verifies that the security-uninitialized device named in the certificate is a member of the trust group of devices referred to by the group name" in (Col 4 line 57 to Col 5 line 21).

Allowable Subject Matter

8. Claims 2-12 are allowed.

Response to Arguments

9. Applicant's amendment, filed on Oct. 05, 2007, has claims 1-2, 13, and 19.

10. Applicant's remark, filed on Oct. 05, 2007, argues that the rejection does not demonstrate a prima facie case of obviousness over the combination for the newly amended independent claim 13.

11. Applicant's remark has been fully considered, but found not persuasive based on the reason below.

Regarding to Argument (1):

In regards to Applicant's argument that the rejection does not demonstrate a prima facie case of obviousness over the combination of cited references, Examiner respectfully disagrees with it. The newly amended claim limitation, "the branding device having previously generated the branding public key and trust group membership certificates", presented in Claim 13 is taught by Dondeti (see lines 14-29, Col. 5 from Dondeti; where the certificate is generated by the host itself). In response to applicant's argument that the action does not demonstrate a prima facie case of obviousness over the combination, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references

themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, since the cited prior art by Hind and Dondeti both disclose the use of certificate for authentication/verification purpose any one of ordinary skill in the art at the time of invention was made to combine the teachings. The motivation for doing so would be to implement the group joining between group members without interposing a central authority as supported by the disclosure from Dondeti that centralized flat scheme consist of a single entity distributing the encryption keys (i.e., central authority) to the group members ... Thus these schemes suffer from the 1 affects n scalability problem (lines 54-58, Col. 1). Therefore, the previously cited prior art is still sufficient to meet the newly amended independent claim 13.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

    a. Caronni et al. (U.S. Patent 6,049,878) disclose a system for secure multicast including at least one sending entity operating on a sending computer system, the sending entity with a sending multicast application running on the sending computer system. A number of receiving entities each running on a receiving computer system, the receiving entities having a receiving multicast application running. A traffic distribution

component coupled to the sending entity and each of the receiving entities, where the traffic distribution component supports a connectionless datagram protocol. A participant key management component operates within each receiver entity where the participant key management component holds a first key that is shared with the sender and all of the receiving entities, and a second key that is shared with the sender and at least one but less than all of the receiving entities. A group key management component is coupled to the traffic distribution component and includes a data structure for storing all of the participant first and second keys.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Y.C. Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Y.C. Shaw
Examiner
Art Unit 2135

THANHNGA TRUONG
PRIMARY EXAMINER